DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: TOP SECRET

b. LEVEL OF SAFEGUARDING REQUIRED: TOP SECRET

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

	a. PRIME CONTRACT NUMBER		
	b. SUBCONTRACT NUMBER		
X	c. SOLICITATION OR OTHER NUMBER: PRDA 02-16-SNK	DUE Date *(YYMMDD)*: 2 08 05	

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

X	a. ORIGINAL *(Complete date in all cases)*		Date *(YYMMDD)*: 2 06 11
	b. REVISED *(Supersedes all previous specs)*	Revision No.	Date *(YYMMDD)*
	c. FINAL *(Complete Item 5 in all cases)*		Date *(YYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? [ ] YES [X] NO. If Yes, complete the following:

Classified material received or generated under _____ *(Preceding Contract Number)* is transferred to this follow-on contract

5. IS THIS A FINAL DD FORM 254? [ ] YES [X] NO. If Yes, complete the following:

In response to the contractor's requested dated _____, retention of the identified classified material is authorized for the period of _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
Reference Source List	See 6a	See 6a

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
N/A	N/A	N/A

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
N/A	N/A	N/A

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Synthetic Aperture LIDAR for Technical Imaging (SALTI). This program will develop a flight-qualified, proof-of-concept laser sensor and associated ground data processing which generates high resolution 2-D and 3-C imagery.

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	X	
b. RESTRICTED DATA		X
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X
d. FORMERLY RESTRICTED DATA		X
e. INTELLIGENCE INFORMATION		
(1) Sensitive Compartmented Information (SCI)		X
(2) Non-SCI		X
f. SPECIAL ACCESS INFORMATION		X
g. NATO INFORMATION		X
h. FOREIGN GOVERNMENT INFORMATION		X
i. LIMITED DISSEMINATION INFORMATION		X
j. FOR OFFICIAL USE ONLY INFORMATION	X	
k. OTHER *(Specify)*		

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		X
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X	
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	X	
e. PERFORM SERVICES ONLY		X
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S. PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	X	
h. REQUIRE A COMSEC ACCOUNT		X
i. HAVE TEMPEST REQUIREMENTS	X	
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		X
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X
l. OTHER *(Specify)* Pre-contract award access to classified is required.	X	

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate Government authority. Proposed public releases shall be submitted for approval prior to release

[ ] Direct [X] Through *(Specify):*

ASC/PA
1865 4th Street, Suite 15
WPAFB, OH 45433-6503

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs) for review.
In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance need for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guidelines/extracts reference herein. Add additional pages as needed to provide complete*

The National Industrial Security Program Operating Manual (NISPOM), Jan 95, applies to this solicitation..

a. Ref Blk 1a: The contractor must be granted a TOP SECRET facility clearance prior to being granted access to TOP SECRET information.

b. Ref Blk 1b: Contractor must obtain TOP SECRET safeguarding capability prior to being provided TOP SECRET information.

c. Ref Blk 10a: COMSEC and/or cryptographic requirements apply. See DoD 5220.22-A.

d. Ref Blk 10j: For Official Use Only (FOUO) applies. See addendum.

e. Ref Blk 11c: Any classified information generated in the performance of this contract shall require the contractor to apply derivative classification and markings consistent with the source material or be governed by the following Security Classification Guide (SCG): EO Targeting Sensors SCG, dated 20 Feb 02, OPR: AFRL/SNJ, WPAFB OH. Special considerations apply. See addendum.

f. Ref Blk 11d: The contractor is required to provide adequate and approved storage for classified hardware or material to the level of SECRET, which because of size or quantity cannot be safeguarded in an approved storage container.

g. Ref Blk 11i: EMSEC Requirement will apply. See addendum.

h. Contract Monitor: Mark A. Bicknell, AFRL/SNJM, (937) 255-5922, ext. 270.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. *(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed)* [ ] Yes [X] No

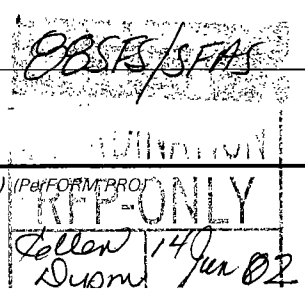
15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. *(If Yes, identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)* [ ] Yes [X] No

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*
Sharma S. Wilkins	Contracting Officer	(937) 255-4279

d. ADDRESS *(Include Zip Code)*	17. REQUIRED DISTRIBUTION	
AFRL/SNKR 2310 Eighth Street, Bldg 167 WPAFB OH 45433-7801	[X]	a. CONTRACTOR
	[ ]	b. SUBCONTRACTOR
	[X]	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
e. SIGNATURE	[ ]	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	[ ]	e. ADMINISTRATION CONTRACTING OFFICER
	[ ]	f. OTHERS AS NECESSARY

DD Form 254, DEC 90 *(REVERSE) (EF-V1)* (PerFORM PRO)



ADDENDUM TO DD FORM 254 (Block 10j)
FOR OFFICIAL USE ONLY (FOUO)
(Reference DoD Regulation 5400.7/Air Force Supplement, 22 July 1999.)

1. **GENERAL**: FOUO is information that has not been given a security classification pursuant to the criteria of an Executive Order, but which may be withheld from the public because disclosure would cause a foreseeable harm to an interest protected by one or more of the Freedom of Information Act (FOIA) exemptions 2 through 9. Additional information on FOUO may be obtained by contacting the User Agency. FOUO is assigned to information at the time it is created in a DoD Agency or derivatively as instructed in a Security Classification Guide.

2. **MARKING**:

a. FOUO information received **(released by a DoD component)** should contain the following marking, when received: ***THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER FOIA. EXEMPTION(S) ___ APPLIES/APPLY.***

b. Mark an unclassified document containing FOUO information "FOR OFFICIAL USE ONLY" at the bottom of each page containing FOUO information and on the bottom of the front page or front cover (if any) and on the back of the last page and on the back cover (if any). Each paragraph containing FOUO information shall be marked as such.

c. Within a classified document, an individual page that contains both FOUO and classified information shall be marked at the top and bottom with the highest security classification of information appearing on the page. Individual paragraphs shall be marked at the appropriate classification level, as well as unclassified or FOUO, as appropriate. An individual page that contains FOUO information but no classified information shall be marked "FOR OFFICIAL USE ONLY" at the top and bottom of the page, as well as each paragraph that contains FOUO information. NOTE: For "production efficiency" the entire document may be marked top and bottom with the highest level of classification contained within it, as long as every paragraph is marked to reflect the specific classification of the information it contains.

d. Mark other records, such as computer print outs, photographs, films, tapes, or slides 'FOR OFFICIAL USE ONLY" so that the receiver or viewer knows the record contains FOUO information.

e. Mark each part of a message that contains FOUO information. Unclassified messages containing FOUO information must show the abbreviation "FOUO" before the text begins.

3. **DISSEMINATION**: FOUO may be disseminated between officials of DoD Components, DoD contractors, consultants and grantees to conduct official business for DoD. Recipients shall be made aware of the status of such information **and transmission shall be by means that preclude unauthorized public disclosure**.

4. **TRANSMISSION**: FOUO information shall be transmitted in a manner that prevents disclosure of the contents. When not commingled with classified information, it may be sent via first-class mail or parcel post. Bulky shipments, i.e. testing materials, that otherwise qualify under postal regulations, may be sent by fourth-class mail. FOUO information may also be sent over facsimile equipment; however, when deciding whether to use this means, balance the sensitivity of the records against the risk of disclosure. Consider the location of sending and receiving machines and ensure authorized personnel are available to receive the FOUO information as soon as it is transmitted. Transmittal documents shall call attention to the presence of FOUO attachments. FOUO information may also be sent via e-mail, if it is sent via a system that will prevent unintentional or unauthorized disclosure.

5. **STORAGE**: To safeguard FOR OFFICIAL USE ONLY records during normal duty hours, place them in an out-of-sight location if your work area is accessible to persons who do not have a valid need for the information. After normal duty hours, store FOUO records to prevent unauthorized access. File them with other unclassified records in unlocked files or desks when normal internal building security is provided. When there is no internal building security, locked buildings or rooms normally provide adequate after-hours protection. If such protection is not considered adequate, FOUO material shall be stored in locked containers such as file cabinets, desks, or bookcases. *Expenditure of funds for security containers or closed areas solely for the protection of FOUO data is prohibited.*

6. **DESTRUCTION**: When no longer needed, FOUO information shall be disposed of by any method that will preclude its disclosure to unauthorized individuals.

ADDENDUM TO DD FORM 254 (Block 11c)
SPECIAL CONSIDERATIONS
(AFMAN 33-214V EXTRACT)

3.4. Special Items. People may innocently introduce other radio devices, such as pagers, hand-held portable transceiver radios, cellular telephones, cordless telephones, and cordless microphones into the area processing classified information with disastrous results. Also, alarm systems may use radio transmitters to alert remotely located security or fire-fighting teams.

3.4.1. Hand-Held Radios. These countermeasures are required. Hand-held radio transceivers used with intrabase radios and land mobile radios deserve special consideration because of their unique operational applications. A person may carry these devices into an area where classified information is processed. If the person carrying such a device works in the facility, either turn off the device and use the telephone or separate it 2 meters from classified processors: no transmissions are allowed. If the person carrying the device is a short-term visitor, it is not necessary to turn off the radio because the visitor usually moves about in the facility. Infrequent transmissions are allowed, but only for short durations.

3.4.2. Beepers and Pagers. These countermeasures are required Beepers and pagers deserve special consideration because of their unique operational applications. A person may carry these devices into an area where classified information is processed. If the person carrying such a device works in the facility, either turn off the device and use the telephone or keep the device 2 meters from classified processors. If the person carrying the device is a short-term visitor, it is not necessary to turn off the device because the visitor usually moves about in the facility. If the device has a transmit capability, follow the instructions for hand-held radios.

3.4.3. Alarm Systems. These countermeasures are required The mode of operation of alarm systems radio frequency transmitters will determine their treatment. Any such transmitter with a continuous transmit mode or a high duty cycle (transmits most of the time) must meet the same separation requirements as all other fixed transmitters; follow the applicable guidance in paragraph **3.3.** If they do not meet these requirements, exclude them from operating in the classified information processing area. Low duty cycle (transmits short bursts infrequently) systems are not considered hazards and require no special treatment.

3.4.4. Cellular Telephones. These countermeasures are required. When a cellular telephone is used as an operational necessity separate it 5 meters from RED equipment. When the cellular telephone is a personal asset, its use is prohibited. Disable the unit from receiving calls or separate it 10 meters from RED processors. Cellular telephones are excluded from operating within 10 meters of the classified information processing area when the facility is located outside the United States.

3.4.5. Cordless Telephones. These countermeasures are required. When a radio frequency cordless telephone is used as an operational necessity, separate it 5 meters from RED equipment. When the cordless telephone is a personal asset, its use is prohibited. Disable the personal cordless telephone from receiving calls or separate it 10 meters from RED processors. There are no separation requirements for infrared cordless telephones. Cordless telephones are excluded from operating within 10 meters of the classified information processing area when the facility is located outside the United States.

3.4.6. Cordless Microphones.

3.4.6.1. Radio Frequency Cordless Microphones. These countermeasures are required. When a radio frequency cordless microphone, encrypted or unencrypted, is used for briefing either classified information or unclassified information, separate it 10 meters from RED equipment. Using unencrypted radio frequency cordless microphones for classified briefings is prohibited.

3.4.6.2. Infrared Cordless Microphones. These countermeasures are required. Using an infrared cordless microphone for briefing classified information requires blocking the line of sight to a possible place where an adversary could detect the infrared emanations. Do not forget that smooth or shiny surfaces cause infrared signals to be reflected. The best solution is to use a closed room, keeping the doors closed and covering the windows with drapes.

3.4.7. Cordless Accessories. These countermeasures are required. When a radio frequency cordless accessory such as a keyboard or a mouse is used, separate it 5 meters from RED equipment. Radio frequency cordless accessories cannot be used to process classified information unless encrypted.

3.4.8 Wireless Local Area Networks (LAN). These countermeasures are required. When a radio frequency wireless LAN is used, separate the transmitter and receiver units 5 meters from RED equipment.

3.4.9 Infrared LANs. These countermeasures are required. An infrared LAN processing classified information requires blocking the line of sight to a possible place where an adversary could detect the infrared emanations Do not forget that smooth or shiny surfaces cause infrared signals to be reflected. The best solution is to use a closed room, keeping the doors closed and covering the windows with drapes.

3.4.10 Infrared Devices. These countermeasures are required. Infrared devices not covered by any subparagraph of paragraph **3.4** requires blocking the line of sight to a possible place where an adversary could detect the infrared emanations Do not forget that smooth or shiny surfaces cause infrared signals to be reflected. The best solution is to use a closed room, keeping the doors closed and covering the windows with drapes.

NOTE: If guidance in paragraph 3.3 on Alarm signals is needed, please contact the Program Manager/Contract Monitor to obtain.

ADDENDUM TO DD FORM 254 (Block 11i)
EMISSION SECURITY (EMSEC) REQUIREMENTS
(FORMERLY TEMPEST REQUIREMENTS)

EMISSIONS SECURITY ASSESSMENT REQUEST (ESAR)

FOR *ALL* CLASSIFIED SYSTEMS

1. The contractor shall ensure that compromising emanations (EMSEC) conditions related to this contract are minimized.

2. The contractor shall provide countermeasure assessment data to the Contracting Officer (CO), in the form of an ESAR. The ESAR shall provide only specific responses to the data required in paragraph 3 below. The contractor's standard security plan shall **NOT** be used as a "stand-alone" ESAR response. The contractor shall **NOT** submit a detailed facility analysis/assessment. The ESAR information will be used to complete an EMSEC Countermeasures Assessment Review of the contractor's facility to be performed by the government EMSEC authority using current Air Force EMSEC directives. EMSEC is applied on a case-by-case basis and further information may be required to complete the review. The contractor shall provide this information to the CO when requested. After the evaluation of the ESAR by the government EMSEC authority, additional EMSEC requirements may be necessary. When changes to the information required in paragraph 3 below occurs (including, but not limited to, relocation, additions, or deletions of equipment from the original approved room), the contractors shall notify the CO of these changes. Upon request, the contractor shall submit to the CO a new ESAR, identifying the new configuration at least 30 days before the change occurs. The contractor shall **NOT** commence processing with the new configuration until receiving, as a minimum, interim approval from the CO.

3. *ESAR contents shall include, as a minimum, the following information:
   a. The specific classification and special categories of material to be processed/handled by electronic means. Include percentage of each classification level used including unclassified (i.e., 5% Top Secret, 10% Secret/SAR, 25% Secret, 60% Unclassified).
   b. The specific location (complete address, building/room number, or office) where classified processing will be performed. Include identification of any other contractor/company located within 200 meters of the facility.
   c. Attach a copy of the Defense Investigative Service (DIS) Form 147 to validate physical security and approved storage level of the facility.
   d. Provide the name, title, and telephone number (commercial and/or DSN) of a point of contact at the facility where processing will occur.

4. The prime contractor shall ensure that all subcontractors and/or vendors comply with EMSEC requirements when performing classified processing related to this contract. The subcontractor will provide the above documentation through their prime to the CO to complete the ESAR.

5. In addition to the information required for all classified systems, the following will be required for **Top Secret** processing:

   a. Identify the radius (in meters) of the physical control space available around the system, equipment, or facility. Describe the barriers, doors, fences, walls, etc that define the area. Describe the control exercised over the area during duty and nonduty hours. Describe other factors, which contribute to control (i.e., visitor procedures, escort requirements, searches of personnel and/or vehicles, etc).

   b. Identify the type and location (relative to the classified system) of any unfiltered/telephone or communication lines, shielded or unshielded twisted pair cables or fiber, underground or unfiltered power lines, conduit, heating and air conditioning ducts, water pipes, etc, that transgress the established controlled area.

   c. Describe the building in which the classified system(s) is housed, i.e., concrete block outer walls, 2" X 4" and single ply gypsum board inner walls, true floor to true ceiling walls, metallic (steel) or solid wood doors, windows (if there are windows, describe the type of coverings on them), etc.

   d. Diagrams and/or drawings would be extremely helpful.

6. Additional information may be requested upon review of the documentation provided.

***NOTE: A copy of your Automated Information System Security Plan(s) (AISSP) will suffice.**